

Marlene H. Dortch, Secretary  
Federal Communications Commission  
Office of the Secretary  
445 12th Street, SW  
Washington, DC 20554

**Annual 47 C.F.R. § 64.2009(e) CPNI Certification**

**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2008

Date filed: February 22, 2008

Name of company covered by this certification: Wisconsin Independent Network, LLC

Form 499 Filer ID: 821874

Name of signatory: Scott A. Hoffmann

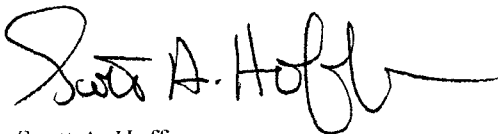
Title of signatory: Executive Director

I, Scott A. Hoffmann, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See 47 C.F.R. § 64.2001 et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).



Scott A. Hoffmann  
Executive Director  
Wisconsin Independent Network, LLC

**Wisconsin Independent Network, LLC**

**STATEMENT EXPLAINING HOW THE COMPANY'S OPERATING PROCEDURES  
ENSURE COMPLIANCE WITH THE FCC'S CPNI RULES**

**I. Customer Proprietary Network Information ("CPNI")**

CPNI is defined in Section 222(f) of the Communications Act as (A) information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier (except that CPNI does not include subscriber list information).

Generally, CPNI includes personal information regarding a consumer's use of his or her telecommunications services. CPNI encompasses information such as: (a) the telephone numbers called by a consumer; (b) the telephone numbers calling a customer; (c) the time, location and duration of a consumer's outbound and inbound phone calls, and (d) the telecommunications and information services purchased by a consumer.

Call detail information (also known as "call records") is a category of CPNI that is particularly sensitive from a privacy standpoint and that is sought by pretexters, hackers and other unauthorized entities for illegitimate purposes. Call detail includes any information that pertains to the transmission of a specific telephone call, including the number called (for outbound calls), the number from which the call was placed (for inbound calls), and the date, time, location and/or duration of the call (for all calls).

**II. Use and Disclosure of CPNI Is Restricted**

The Company recognizes that CPNI includes information that is personal and individually identifiable, and that privacy concerns have led Congress and the FCC to impose restrictions upon its use and disclosure, and upon the provision of access to it by individuals or entities inside and outside the Company.

The Company has designated a CPNI Compliance Officer who is responsible for: (1) communicating with the Company's attorneys and/or consultants regarding CPNI responsibilities, requirements and restrictions; (2) supervising the training of Company employees and agents who use or have access to CPNI; (3) supervising the use, disclosure, distribution or access to the Company's CPNI by independent contractors and joint venture partners; (4) maintaining records regarding the use of CPNI in marketing campaigns; and (5) receiving, reviewing and resolving questions or issues regarding use, disclosure, distribution or provision of access to CPNI.

Company employees and agents that may deal with CPNI have been informed that there are substantial federal restrictions upon CPNI use, distribution and access. In order to be authorized to use or access the Company's CPNI, employees and agents must receive training with respect to the requirements of Section 222 of the Communications Act and the FCC's CPNI Rules (Subpart U of Part 64 of the FCC Rules).

Before an agent, independent contractor or joint venture partner may receive or be allowed to access or use the Company's CPNI, the agent's, independent contractor's or joint venture partner's agreement with the Company must contain provisions (or the Company and the agent, independent contractor or joint venture partner must enter into an additional confidentiality agreement which provides) that: (a) the agent, independent contractor or joint venture partner may use the CPNI only for the purpose for which the CPNI has been provided; (b) the agent, independent contractor or joint venture partner may not disclose or distribute the CPNI to, or allow access to the CPNI by, any other party (unless the agent, independent contractor or joint venture partner is expressly and specifically required to do so by a court order); and (c) the agent, independent contractor or joint venture partner must implement appropriate and specific safeguards acceptable to the Company to ensure the confidentiality of the Company's CPNI.

### **III. Protection of CPNI**

1. The Company may, after receiving an appropriate written request from a customer, disclose or provide the customer's CPNI to the customer by sending it to the customer's address or record. Any and all such customer requests: (1) must be made in writing; (2) must include the customer's correct billing name and address and telephone number; (3) must specify exactly what type or types of CPNI must be disclosed or provided; (4) must specify the time period for which the CPNI must be disclosed or provided; and (5) must be signed by the customer. The Company will disclose CPNI upon affirmative written request by the customer to any person designated by the customer, but only after the Company calls the customer's telephone number of record and/or sends a notification to the customer's address of record to verify the accuracy of this request.
2. The Company will provide CPNI to a law enforcement agency in accordance with applicable legal requirements.
3. The Company is a carrier's carrier which does not generate, receive, use or distribute call detail information. Since it does not have call detail information, the Company has not implemented a password system to protect such information.
4. Since December 8, 2007, Company employees authenticate all telephone requests for CPNI in the same manner. That is, Company employees must: (a) send the requested information to the customer's postal or electronic "address of record" (see definition above); or (b) call the customer back at the customer's "telephone number of record" (see definition above) with the requested information.

5. The Company has adopted a policy that it does not and will not use, disclose or permit access to CPNI by an affiliate.

6. When an existing customer calls the Company to inquire about or order new, additional or modified services (in-bound marketing), the Company may use the customer's CPNI other than call detail CPNI to assist the customer for the duration of the customer's call if the Company provides the customer with the oral notice required by Sections 64.2008(c) and 64.2008(f) of the FCC's Rules and after the Company authenticates the customer.

7. The Company has adopted a policy that it does not and will not use, disclose, or permit access to CPNI in connection with Company-initiated marketing of services to which a customer does not already subscribe from the Company (out-bound marketing).

8. If it ever uses CPNI for out-bound marketing, the Company will maintain appropriate paper and/or electronic records that allow its employees, independent contractors and joint venture partners to clearly establish the status of each customer's Out-out and/or Opt-In approvals (if any) prior to use of the customer's CPNI. These records will include: (i) the date(s) of any and all of the customer's deemed Opt-out approvals and/or Opt-in approvals, together with the dates of any modifications or revocations of such approvals; and (ii) the type(s) of CPNI use, access, disclosure and/or distribution approved by the customer.

9. Before a customer's CPNI can be used in an out-bound marketing activity or campaign, the Company's records will be checked to determine the status of the customer's CPNI approval. Company employees, independent contractors and joint venture partners are required to notify the CPNI Compliance Officer of any access, accuracy or security problems they encounter with respect to these records.

If new, additional or extended approvals are necessary, the CPNI Compliance Officer will determine whether the Company's "Opt-Out CPNI Notice" or "Opt-In CPNI Notice" must be used with respect to various proposed out-bound marketing activities.

10. The CPNI Compliance Officer will maintain a record of each out-bound marketing activity or campaign, including: (i) a description of the campaign; (ii) the specific CPNI that was used in the campaign; (iii) the date and purpose of the campaign; and (iv) what products and services were offered as part of the campaign. This record shall be maintained for a minimum of one year.

11. The Company's employees and billing agents may use CPNI to initiate, render, bill and collect for telecommunications services. The Company may obtain information from new or existing customers that may constitute CPNI as part of applications or requests for new, additional or modified services, and its employees and agents may use such customer information (without further customer approval) to initiate and provide the services. Likewise, the Company's employees and billing agents may use customer service and calling records (without customer approval): (a) to bill customers for services rendered to them; (b) to investigate and resolve disputes with customers regarding their bills; and (c) to pursue legal, arbitration, or other processes to collect late or unpaid bills from customers.

12. The Company's employees and agents may use CPNI without customer approval to protect the Company's rights or property, and to protect users and other carriers from fraudulent, abusive or illegal use of (or subscription to) the telecommunications service from which the CPNI is derived.

Because allegations and investigations of fraud, abuse and illegal use constitute very sensitive matters, any access, use, disclosure or distribution of CPNI pursuant to this Section must be expressly approved in advance and in writing by the Company's CPNI Compliance Officer.

13. The Company's employees, agents, independent contractors and joint venture partners may **NOT** use CPNI to identify or track customers who have made calls to, or received calls from, competing carriers. Nor may the Company's employees, agents, independent contractors or joint venture partners use or disclose CPNI for personal reasons or profit.

14. Company policy mandates that files containing CPNI be maintained in a secure manner such that they cannot be used, accessed, disclosed or distributed by unauthorized individuals or in an unauthorized manner.

15. Paper files containing CPNI are kept in secure areas, and may not be used, removed, or copied in an unauthorized manner.

16. Company employees, agents, independent contractors and joint venture partners are required to notify the CPNI Compliance Officer of any access or security problems they encounter with respect to files containing CPNI.

17. Since December 8, 2007, the Company will notify customers immediately of certain changes in their accounts that may affect privacy or security matters.

a. The types of changes that require immediate notification include: (a) change or request for change of the customer's password; (b) change or request for change of the customer's address of record; (c) change or request for change of any significant element of the customer's online account; and (d) a change or request for change to the customer's responses with respect to the back-up means of authentication for lost or forgotten passwords.

b. The notice may be provided by: (a) a Company call or voicemail to the customer's telephone number of record; (b) a Company text message to the customer's telephone number of record; or (c) a written notice mailed to the customer's address of record (to the customer's prior address of record if the change includes a change in the customer's address of record).

c. The notice must identify only the general type of change and must not reveal the changed information.

18. Since December 8, 2007, the Company must provide an initial notice to law enforcement and a subsequent notice to the customer if a security breach results in the disclosure of the customer's CPNI to a third party without the customer's authorization.

a. As soon as practicable (and in no event more than seven (7) days) after the Company discovers that a person (without authorization or exceeding authorization) has intentionally gained access to, used or disclosed CPNI, the Company must provide electronic notification of such breach to the United States Secret Service and to the Federal Bureau of Investigation via a central reporting facility accessed through a link maintained by the FCC at <http://www.fcc.gov/eb/cpni>.

19. Since December 8, 2007, the Company takes reasonable measures to discover and protect against activity that is indicative of pretexting including requiring Company employees, agents, independent contractors and joint venture partners to notify the CPNI Compliance Officer immediately by voice, voicemail or email of: (a) any suspicious or unusual call requesting a customer's call detail information or other CPNI (including a call where the caller furnishes an incorrect password or incorrect answer to one or both of the "shared secret" question-answer combinations); (b) any suspicious or unusual attempt by an individual to change a customer's password or account information (including providing inadequate or inappropriate identification or incorrect "address or record," "telephone number of record" or other significant service information); (c) any and all discovered instances where access to the Company's electronic files or databases containing passwords or CPNI was denied due to the provision of incorrect logins and/or passwords; and (d) any complaint by a customer of unauthorized or inappropriate use or disclosure of his or her CPNI. The CPNI Compliance Officer will request further information in writing, and investigate or supervise the investigation of, any incident or group of incidents that reasonably appear to entail pretexting.

#### **IV. CPNI Compliance Officer**

In addition to the specific matters required to be reviewed and approved by the Company's CPNI Compliance Officer, employees and agents, independent contractors and joint venture partners are strongly encouraged to bring any and all other questions, issues or uncertainties regarding the use, disclosure, or access to CPNI to the attention of the Company's CPNI Compliance Officer for appropriate investigation, review and guidance. The extent to which a particular employee or agent brought a CPNI matter to the attention of the CPNI Compliance Officer and received appropriate guidance is a material consideration in any disciplinary action brought against the employee or agent for impermissible use, disclosure or access to CPNI.

#### **V. Disciplinary Procedures**

The Company has informed its employees and agents, independent contractors and joint venture partners that it considers compliance with the Communications Act and FCC Rules regarding the use, disclosure, and access to CPNI to be very important.

Violation by Company employees or agents of such CPNI requirements will lead to disciplinary action (including remedial training, reprimands, unfavorable performance reviews, probation, and termination), depending upon the circumstances of the violation (including the severity of the violation, whether the violation was a first time or repeat violation, whether appropriate guidance was sought or received from the CPNI Compliance Officer, and the extent to which the violation was or was not deliberate or malicious).

Violation by Company independent contractors or joint venture partners of such CPNI requirements will lead to prompt disciplinary action (up to and including remedial training and termination of the contract).

**Wisconsin Independent Network, LLC**

**STATEMENT OF ACTIONS TAKEN AGAINST DATA BROKERS**

- A. During Calendar Year 2007, the Company has instituted the following proceeding, or filed the following petitions, against data brokers before the Federal Communications Commission:

NONE

- B. During Calendar Year 2007, the Company has instituted the following proceeding, or filed the following petitions, against data brokers before the following state public service commission:

NONE

- C. During Calendar Year 2007, the Company has instituted the following proceeding, or filed the following petitions, against data brokers before the following federal or state courts:

NONE



**Wisconsin Independent Network, LLC**

**SUMMARY OF CUSTOMER COMPLAINTS  
REGARDING UNAUTHORIZED RELEASE OF CPNI**

- A. During Calendar Year 2007, the Company has received the following number of customer complaints related to unauthorized access to, or disclosure of, CPNI due to improper access by Company employees:

NONE

- B. During Calendar Year 2007, the Company has received the following number of customer complaints related to unauthorized access to, or disclosure of, CPNI due to improper disclosure to individuals not authorized to receive the information:

NONE

- C. During Calendar Year 2007, the Company has received the following number of customer complaints related to unauthorized access to, or disclosure of, CPNI due to improper access to online information by individuals not authorized to view the information:

NONE

- D. During Calendar Year 2007, the Company has become aware of the following processes that pretexters are using to attempt to access its CPNI:

NONE